

Amendments to the Specification:

Please replace the paragraph that begins on page 11 line 236 to page 12, line 252 with the following paragraphs:

After receiving the file 50, the signatory 40 analyzes the file 50 and detects if there is any virus infection or intrusion. The signatory 40 then generates a digital signature chain 55 (e.g., a digital signature) that verifies the integrity of the file 50, and returns the digital signature chain 55 back to the requesting platform 35₁. When there are many files to be checked, there may be a need to identify which file the signatory 40 is associated with. The signatory 40, therefore, may contain a file identifier so that the requesting platform 35₁ can know which file the signatory 40 is associated with.

Referring now to Figure 3, one exemplary embodiment of a verification scheme performed by the requesting platform 35₁ to verify that the signatory 40 failed to detect an abnormality in the uploaded file 50 is shown. Upon receipt of the digital signature chain 55, namely a digital signature for clarity sake, the platform 35₁ recovers contents of the digital signature. The recovered contents of the digital signature include a digest 200 of the uploaded file. In addition, the file 50 undergoes a hash function 210 to produce a digest 220. If the digest 210 matches the recovered digest 200, the integrity of the file 50 has been verified and the platform 35₁ allows the file to be opened and/or executed.

Please replace the paragraph that begins on page 16 lines 343-353 (1-11) with the following paragraph:

In particular, the file analyzer 700 is a facility to perform scan operations on the original file ~~265-50~~ and return the scanned file ~~280~~720. The scan operations include, but are not limited or restricted to a virus detection, an intrusion detection, a file integrity detection, or any appropriate program. The virus detection may be a commercial anti-virus program or virus scanner such as the MCAFEE® virus scanner, or an intrusion detector based on an expert system

or an artificial immune system. The file analyzer 700 generates the scanning result 730 according to the result of the scan. The scanning result 730 may indicate that the original file 50 has an acceptable file integrity (e.g., virus free), an unacceptable file integrity (e.g., infected with virus), or a questionable integrity which may require in-person analysis of the file.

Please replace the paragraph that begins on page 16 lines 354-357 (12-15) with the following paragraph:

The signature generator 710 receives the scanned file 720 and ~~optimally~~optionally the result 730 (represented by dashed lines). Thereafter, the signature generator 710 produces a digital signature 740. The digital signature 740 may be part of the digital signature chain 55, described above.

Please replace the paragraph that begins on page 16 lines 358-363 with the following paragraphs:

It is further contemplated that the file checker 45 is optimally implemented with a time stamp indicator 750. The time stamp indicator 750 provides information regarding the recency of the scan operation. In one embodiment, the time stamp indicator 750 is one of a calendar time obtained from the platform.

Figure 8 is a flowchart illustrating a process 800 for remote file checking according to one embodiment of the invention.